UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

| | | |
|---|---|---|
| UNITED STATES OF AMERICA, | ) | |
| | ) | 4:16CR374 JAR/PLC |
| Plaintiff, | ) | |
| | ) | |
| v. | ) | DECLARATION OF MICHELE BUSH |
| | ) | |
| ROLAND HOEFFENER | ) | |
| | ) | |
| Defendant. | ) | |

I, MICHELE BUSH, hereby declare as follows:

1. I am a computer forensics expert at Loehrs & Associates, LLC, (formerly Law2000, Inc.) a firm specializing in computer forensics, located at 3037 West Ina, Suite 121, Tucson, Arizona 85741. I am competent to testify and the matters contained herein are based on my own personal knowledge

2. I hold Associate Degrees in Arts and Science and Bachelor Degree of Science in Psychology. I have completed numerous hours of forensics training including courses with Guidance Software and Access Data. I am an EnCase Certified Examiner (EnCE), Certified Computer Examiner (CCE), and Access Data Certified Examiner (ACE). I have conducted hundreds of forensics exams on hundreds of pieces of evidence including hard drives, cell phones, removable storage media and other electronic devices. In addition, I hold a Private Investigator license in the State of Arizona. A copy of my Curriculum Vitae is attached hereto as Exhibit A.

3. I have been retained as a computer forensics expert consultant by Daniel Juengel and Joe Flees, counsel for Defendant Roland Hoeffener, for the purpose of assisting with matters related to the analysis of electronic evidence in this matter.

4. I have reviewed discovery materials produced by the Government including the Affidavit for Search Warrant prepared by Detective Dustin Partney (Detective Partney), the Regional Computer Crimes Education and Enforcement Group (RCCEEG) forensics report prepared by Officer Steve Grimm dated 08/05/15, the Torrential Downpour log and Indictment.

5. According to the Affidavit for Search Warrant prepared by Detective Partney on April 29, 2013, this case originated on December 15, 2012 when Hoeffener's IP address at the time, 76.215.116.247, was identified as offering a torrent suspected to contain child pornography "while utilizing software configurated to search the BitTorrent network" (page 2). During this investigation, a log file detailing the network activity between law enforcement's software and Mr. Hoeffener's IP address was produced.

6. In reviewing the log file provided by the Government, I noted the software utilized by Detective Partney is identified as Torrential Downpour. This is a modified version of publicly available file sharing software used exclusively by law enforcement. It is my understanding this software has been altered in a way that is different than the public versions in at least three ways: 1) it downloads files from a single IP address, 2), it does not share files, and 3) it creates a detailed log of network activity between the software and the suspect.

7. In order to understand the complexities of the undercover investigation that identified Mr. Hoeffener in this matter, it is imperative to understand the difference between the "BitTorrent network", a "torrent", an "info hash" and an actual image or video that depicts child pornography.

8. The "BitTorrent network" is essentially a protocol or set of rules that allows users to download and upload parts of files from many different users which are then

rebuilt into the whole files. The BitTorrent network tracks users downloading and uploading data and categorizes them as either a "seed" or a "leech". A seed is a client that possesses all parts of a torrent download and allows other users to obtain the data. A leech is a client that is seeking data to download and/or a client that does not contribute to the network by restricting its uploaded data. Clients identified as leeches can eventually be restricted from receiving data, per a "tit-for-tat" policy requiring users to contribute data in order to obtain data. Based on my understanding of Torrential Downpour, the BitTorrent network would identify law enforcement as a "leech" because it does not share data. It is unknown how the BitTorrent protocol affects Torrential Downpour's ability to successfully operate on the network and identify suspects if it flagged as a leech.

9. A "torrent" is a text file proprietary to the BitTorrent network that contains instructions for torrent software, such as uTorrent or BitLord, on how to download a file or sets of files on the BitTorrent network. Torrent files do not contain user data, such as images or videos, but rather an index containing information about the files associated with that torrent including but not limited to, names of the files instructed to download, the torrent author, the date the author of the torrent created the file, the number of files the torrent is set to download, and the URLs tracking the torrent activity. It is unknown if Torrential Downpour can identify a client containing only the torrent of suspect child pornography without possessing its content.

10. An "info hash" is a mathematical algorithm or hash value that uniquely identifies the "torrent" on the BitTorrent network. Although it has been described as synonymous with a fingerprint, the info hash only identifies the torrent itself, not the actual files the torrent would download if parsed. Therefore, identifying a suspect with an info hash of a

torrent of suspect child pornography does not necessarily mean that suspect actually possesses child pornography because no child pornography will exist until the torrent is parsed. It is my understanding Torrential Downpour limits it searches on the network to torrents containing info hash values identified by law enforcement as containing files of suspect child pornography. However, torrents can be responsible for hundreds, if not thousands, of files created in a single download. It is unknown which torrents Torrential Downpour searches for and if a torrent responsible for 99 percent legal pornography and one file of suspected child pornography would be identified.

11. The network log produced by the Torrential Downpour software during this investigation identified the suspect's software application utilized to connect to the BitTorrent network as uTorrent version 2.2.1, the client identifier as 2d5554323231302da162caf3e4dbdd7293c9e5a8, and the port used to communicate as 22679, among additional information. Although this log establishes that a connection was made between the software and the suspect, one must validate the merits of the search warrant by identifying the information reported during the undercover investigation on the evidence seized from the suspect. I have not had the opportunity to examine the digital media seized from Mr. Hoeffener's residence and have relied upon the RCCEEG forensics report prepared on behalf of the government.

12. A review of the RCCEG forensics report revealed an examination was conducted on approximately eight hard drives installed with operating systems. Only two hard drives were found to contain file sharing software including LimeWire and eMule. The report is silent with regard to locating the uTorrent software version 2.2.1, the torrent identified, or the files of suspected child pornography specifically downloaded on any of the evidence items. Further, the majority of the suspect child pornography was located

within system locations on the hard drive, compressed backup files, external devices, and possibly encrypted containers, so it is unknown if any of those locations would have been publicly available. Other than the existence of child pornography, no connection was made between the undercover investigation and evidence seized from Mr. Hoeffener's residence that would indicate he was the suspect identified.

13. In my experience on many cases involving P2P undercover investigations using software developed for law enforcement's use, the very same issues have been raised with regard to the accuracy and reliability of the data reported including whether the automated software is accessing information that is not publicly available. I have conducted forensic exams on computers seized during undercover investigations and found evidence contrary to the information reported by law enforcement's software such as file sharing had been turned off prior to the undercover investigation or that files only existed in private folders that were not available for sharing and should not have been identified by law enforcement's automated software. Similarly in this case, the RCCEEG did not report on locating the file sharing application utilized by the suspect or the torrent reportedly downloaded. Further, no mention was made with regard to files of suspect child pornography being publicly available and shared through the file sharing applications.

14. In my forensic training, some of which has come directly from law enforcement, I have been taught that I cannot rely on a tool (software) that has not been tested and validated by me and is not available for testing and validation by my industry peers. Private and public sector experts utilize the same industry standard tools such as EnCase and Forensic Tool Kit (FTK) to read electronic media and report information from it. The information extracted using these tools is not contested because they are

constantly being tested, validated, and updated by reliable sources to ensure it is reading and reporting information accurately. These tools have been accepted by the Courts as viable tools. However, even those tools have been proven to produce inaccurate and unreliable data at times which has only been discovered through the ability to test, validate, and improve them.

15. The biggest challenge with developing an accurate tool is the diversity of data being collected and analyzed. This is why even tools like EnCase and FTK sometimes produce inaccurate and unreliable results. No two computer systems are identical. Computers are installed with different operating systems and there are hundreds of different versions of the same operating system, some are updated regularly and some are not updated at all. Those operating systems have thousands of different settings that can make each system unique in how it functions and records data. Within those operating systems a user can install millions of different software applications from large commercially produced software to small home-made software applications. Software applications may have bugs, data can be corrupted or incomplete, computers can be infected with viruses, Trojans and other malware. All of these variables have an effect on how that data is collected, analyzed and documented by a tool. While a tool may provide accurate information on an updated Windows system without any malware, the same tool may yield false results on a system that has not been updated and is infested with viruses.

16. When talking specifically about P2P software, there are hundreds of versions of file sharing software applications that users can download from the Internet. Some are free and some are paid for. Some are updated regularly with new versions, some are not. Some of those applications are open source, meaning the user can actually modify

the source code of the application allowing it to function differently than the exact same piece of software installed on another computer. I have personally been researching, testing and analyzing P2P file sharing software available to the public for over ten years including, but not limited to, LimeWire, FrostWire, Bearshare, Ares, BitTorrent, eMule, Phex and Shareaza. What I have discovered in all of these programs is that they can contain bugs, they do not always function as intended and the data reported by these applications is not always accurate or reliable. In that regard, any tool used to collect, analyze and document data associated with these applications may also be inaccurate and unreliable.

17. For all of the reasons stated above, and under general scientific principles, it is my opinion that there is no credible evidence that the files identified as suspect child pornography in Detective Partney's Affidavit for Search Warrant and included as part of Count One of the Indictment were publicly available on the suspect computer identified at IP addresses 76.215.116.247. In addition, it remains my opinion that law enforcement's proprietary software needs to be tested by a qualified third-party to determine its functionality and accuracy.

18. I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

DATED: April 7, 2017

MICHELE BUSH